BOLETIM DE SEGURANÇA

Grupo de ransomware Black Basta associado a ataques zero day no Windows

heimdall
security research
A DIVISION OF ISH

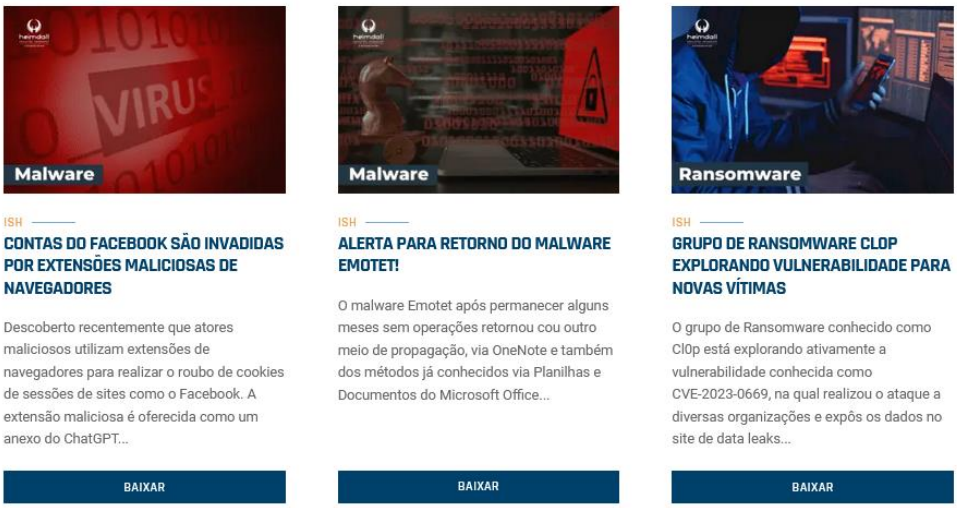
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Recentemente a Symantec identificou que a vulnerabilidade (CVE-2024-26169) classificada como alta, está sendo explorada pelo grupo de cibercriminosos **Cardinal**, também conhecido como **Storm-1811** e **UNC4394**, e pelos operadores da gangue Black Basta. A informação sugere que essa vulnerabilidade pode ter sido explorada como um ataque de zero day.

2 DETALHES SOBRE A VULNERABILIDADE

A vulnerabilidade CVE-2024-26169 foi identificada no serviço de relatório de erros do Windows. Sua exploração em sistemas vulneráveis, pode permitir que um invasor aumente seus privilégios. Em março de 2024, a Microsoft lançou uma correção para essa vulnerabilidade, afirmando naquele momento que não havia indícios de que ela estivesse sendo explorada ativamente. Contudo, uma análise recente de uma ferramenta de exploração usada em ataques mostrou que ela pode ter sido desenvolvida antes da liberação da correção. Isso sugere que pelo menos um grupo de atacantes pode ter se aproveitado dessa vulnerabilidade antes de ser conhecida, caracterizando um ataque de dia zero.

A equipe Threat Hunter da Symantec investigou uma tentativa de ataque de ransomware que utilizou uma ferramenta de exploração específica. Apesar dos invasores não terem conseguido efetivamente implantar o ransomware, as estratégias e técnicas empregadas (conhecidas como TTPs) eram notavelmente parecidas com as descritas em um relatório que a Microsoft recentemente informou sobre as atividades do grupo Black Basta. Isso incluiu a utilização de scripts em lote disfarçados como atualizações de software. Mesmo sem a implantação bem-sucedida de uma carga útil, a similaridade nos TTPs sugere fortemente que este pode ter sido uma tentativa frustrada de ataque pelo grupo Black Basta.

A ferramenta de exploração, ao ser analisada, demonstrou que se beneficia da circunstância em que o arquivo **werkernel.sys** do Windows cria chaves de registro com um descritor de segurança nulo. Dado que a chave mãe possui uma entrada de controle de acesso (**ACE**) “**Creator Owne**” para as subchaves, todas as subchaves serão propriedade dos usuários do processo em execução. A exploração utiliza essa característica para criar uma chave de registro “**HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WerFault.exe**”, onde estabelece o valor “**Debugger**” como o caminho do seu próprio executável. Isso possibilita que o exploit inicie um shell com privilégios de administrador.

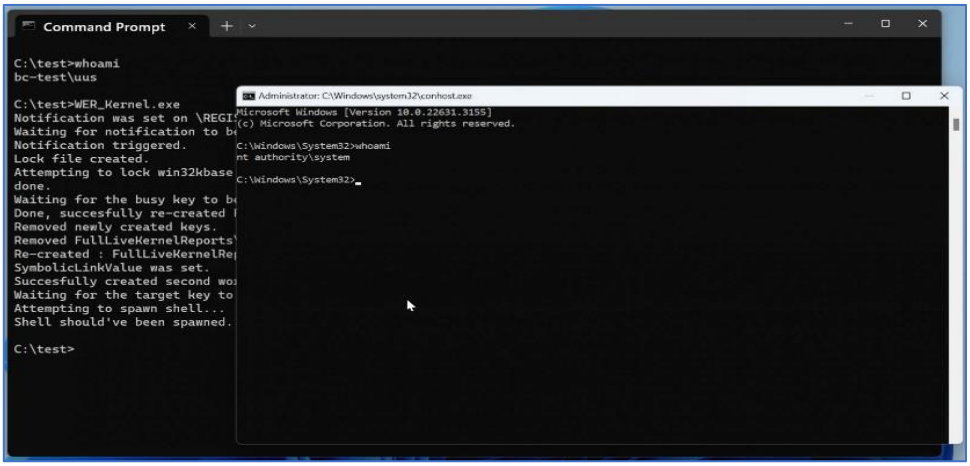


Figura 1 – Demonstração do exploit usado por Black Basta no Windows 11.

A versão da ferramenta utilizada neste ataque apresentava um carimbo de data/hora de compilação de 27 de fevereiro de 2024, algumas semanas antes da correção da vulnerabilidade. Foi descoberta no Virus Total uma segunda versão da ferramenta com um carimbo de data/hora de compilação anterior, de dezembro de 2023.

Os carimbos de data/hora em executáveis portáteis podem ser modificados, o que significa que um carimbo de data/hora não é uma prova definitiva de que os invasores estavam explorando a vulnerabilidade como um dia zero. Contudo, neste caso, parece haver pouca razão para os atacantes alterarem o carimbo de data/hora para uma data anterior.

Em abril de 2022, o Cardinal lançou o Black Basta, um ransomware que, desde o início, manteve uma estreita relação com o botnet Qakbot, aparentemente seu principal meio de infecção. O Qakbot, é um dos botnets mais eficazes na distribuição de malware em todo o mundo, foi desativado após intervenções policiais em agosto de 2023. Isso resultou em uma diminuição na atividade do Black Basta. No entanto, o Cardinal não demorou a retomar os ataques e agora parece ter se aliado aos operadores do carregador DarkGate para acessar possíveis vítimas.

3 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Atualização de segurança

- A Microsoft lançou uma atualização de segurança para proteger os sistemas contra essa vulnerabilidade. É altamente recomendável que os usuários apliquem essa atualização de segurança1.

Verificação regular de atualizações

- Verifique regularmente se há atualizações de segurança e instale-as assim que estiverem disponíveis.

Software antivírus

- Mantenha um software antivírus atualizado em seu sistema para detectar e prevenir ataques maliciosos.

Firewall

- Use um firewall para bloquear conexões não autorizadas.

Privilégios de usuário

- Limite os privilégios de usuário em seu sistema. Apenas usuários autorizados devem ter acesso a funções administrativas.

Backup de dados

- Faça backup regular de seus dados. Em caso de um ataque bem-sucedido, você poderá restaurar seus dados a partir do backup.

Conscientização de segurança

- Eduque-se e aos outros sobre as práticas de segurança cibernética. Isso pode ajudar a prevenir ataques futuros.

4 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso do artefato	
md5:	f17918862a190afd4649b2a6b4a34b5c
sha1:	4ea121b4b45bab1e17fae11c8cce30241f5f8a75
sha256:	b73a7e25d224778172e394426c98b86215087d815296c71a3f76f738c720c1b0
File name:	WER_Kernel.exe

Indicadores de compromisso do artefato	
md5:	acaf01f83da439915027c3e2e900c8dd
sha1:	2861b4e463fa89e05f2d7d629fae5140cef49843
sha256:	3b3bd81232f517ba6d65c7838c205b301b0f27572fcfef9e5b86dd30a1d55a0d
File name:	3b3bd81232f517ba6d65c7838c205b301b0f27572fcfef9e5b86dd30a1d55a0d.bat

Indicadores de compromisso do artefato	
md5:	1984cd0bf7b20c5bef58338f80e4e65e
sha1:	b4b5963c62c07c2adcee093571afd0e9e765de3b
sha256:	2408be22f6184cdccec7a34e2e79711ff4957e42f1ed7b7ad63f914d37dba625
File name:	u0.bat

Indicadores de compromisso do artefato	
md5:	ff217dab57393592c6767de1c6a999eb
sha1:	cc580c52f4263803255d65dfb6ab208be7f4a534
sha256:	b0903921e666ca3ffd45100a38c11d7e5c53ab38646715eafc6d1851ad41b92e
File name:	ScreenConnect.ClientSetup.exe

Tabela 1 – Indicadores de Compromissos de artefatos

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Symantec**
- **Bleepingconputer**
- **NVD**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH